

06-19-00
D. SCOTT HEMINGWAY, P.C.

SUITE 800 • PRESTON PLAZA TOWER
8300 DOUGLAS AVENUE
DALLAS, TEXAS 75225

INTELLECTUAL PROPERTY LAW
PATENTS • COPYRIGHTS • TRADEMARKS
LITIGATION • PROSECUTION • LICENSING

PHONE: (214) 706-9082
FACSIMILE: (214) 706-9085
E-MAIL: SHEMINGWAY@UNICOMP.NET

Via United States Express Mail

June 16, 2000

Assistant Commissioner of Patents
Box PATENT APPLICATION
Washington, DC 20231

Re: New Patent Application Transmittal

Transmitted herewith for filing is the patent application of:

Inventors: Basavaraj B. Patil, Raja P. Narayanan,
Emad A. Qaddoura, and Haseeb Akhtar

For: Security Framework for IP Mobility Systems Using Variable-
Based Security Associations and Broker Redirection

Type: Original

Attorney's

Docket No.: P1003

Enclosed for filing are the following papers relating to the above-identified application for patent:

- Specification (21 pages), Claims (8 pages), and Abstract (1 page)
Total pages: 30
- Combined Declaration and Power of Attorney (4 pages) (unexecuted)
- Informal/Formal Drawings (4 sheets)

"Express Mail" mailing label No. EK767028407US

Date of Deposit: June 16, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Commissioner for Patents, Washington, D.C. 20231

D. Scott Hemingway
(Typed or printed name of person mailing paper or fee)

D. Scott Hemingway
(Signature of person mailing paper or fee)

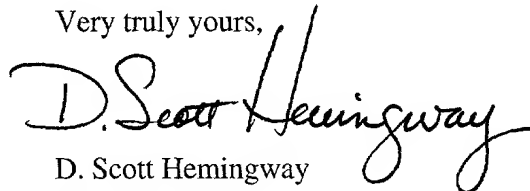
Commissioner of Patents and Trademarks
Box Patent Application
June 16, 2000
Page 2

CLAIMS AS FILED

	Number Filed	Number Extra	Rate	Fee
Total Claims	(37 - 20) =	17	x \$18.00	\$306.00
Independent Claims	(4 - 3) =	1	x \$78.00	\$78.00
Multiple Dependent Claims		0	x \$260.00	
Basic Fee				<u>\$ 690.00</u>
Total Filing Fee				\$1074.00

Please file the application, drawings and record the identification of the inventors. All correspondence should be directed to the Applicant's attorney at the address set forth in the Declaration and Power of Attorney for Patent Application (unexecuted). Enclosed herewith is the above-identified fee. If this fee is insufficient or additional payments are required, please deduct any additional charges from the deposit account for D. Scott Hemingway, Deposit Account No. 501270. Please credit any overpayment to the same deposit account.

Very truly yours,


D. Scott Hemingway
Reg. No. 36,366

Enclosures

**SECURITY FRAMEWORK FOR IP MOBILITY
SYSTEMS USING VARIABLE-BASED
SECURITY ASSOCIATIONS AND BROKER
REDIRECTION**

INVENTORS:

Basavaraj B. Patil
Raja P. Narayanan
Haseeb Akhtar
Emad A. Qaddoura

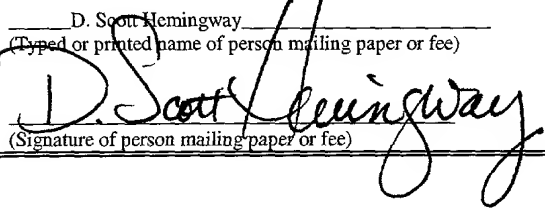
009790-7556563

"Express Mail" mailing label No. EK767028407US

Date of Deposit: June 16, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Commissioner for Patents, Washington, D.C. 20231

D. Scott Hemingway
(Typed or printed name of person mailing paper or fee)


(Signature of person mailing paper or fee)

5

10

15

20

A security framework for an IP-based mobile communication system having a home network, foreign network and a mobile node.

BACKGROUND OF THE INVENTION

Present-day Internet communications represent the synthesis of technical developments begun in the 1960s – the development of a system to support communications between different United States military computer networks, and the subsequent development of a system to support the communication between research computer networks at United States universities. These technological developments would subsequently revolutionize the world of computing.

The Internet, like so many other high tech developments, grew from research originally performed by the United States Department of Defense. In the 1960s, Defense Department officials began to notice that the military was accumulating a large collection of computers - - some of which were connected to large open computer networks and others that were connected to smaller closed computer networks. A network is a collection of computers or computer-like devices communicating across a common transmission medium. Computers on the Defense Department's open computer networks, however, could not communicate with the other military computers on the closed systems.

Defense Department officials requested that a system be built to permit communication between these different computer networks. The Defense Department recognized, however, that a single centralized system would be vulnerable to missile attacks or sabotage. Accordingly, the Defense Department mandated that the system to be used for communication between these military computer networks be decentralized and that no critical services be concentrated in a few, vulnerable failure points. In order to achieve these goals, the Defense Department established a decentralized standard protocol for communication between network computers.

A few years later, the National Science Foundation (NSF) wanted to connect network computers at various research institutions across the country. The NSF adopted the Defense Department's protocol for

communication, and this combination of research computer networks would eventually evolve into the Internet.

Internet Protocols

The Defense Department's communication protocol governing data transmission between computers on different networks was called the Internet Protocol (IP) standard. The IP standard now supports communications between computers and networks on the Internet. The IP standard identifies the types of services to be provided to users, and specifies the mechanisms needed to support these services. The IP standard also describes the upper and lower system interfaces, defines the services to be provided on these interfaces, and outlines the execution environment for services needed in the system.

A transmission protocol, called the Transmission Control Protocol (TCP), was also developed to provide connection-oriented, end-to-end data transmission between packet-switched computer networks. The combination of TCP with IP (TCP/IP) forms a system or suite of protocols for data transfer and communication between computers on the Internet. The TCP/IP standard has become mandatory for use in all packet switching networks that connect or have the potential for utilizing connectivity across network or sub-network boundaries.

The TCP/IP Protocol

In a typical Internet-based communication scenario, data is transmitted from an applications program in a first computer, through the first computer's network hardware, and across the transmission medium to the intended destination on the Internet. After receipt at a destination computer network, the data is transmitted through the destination network to a second computer. The second computer then interprets the communication using the identical protocols on a similar application program. Because of the standard protocols used in Internet communications, the TCP/IP protocol on the second computer decodes the

transmitted information into the original information transmitted by the first computer.

One of the rules in TCP/IP communications is that a computer user does not need to get involved with details of data communication. In order to accomplish this goal, the TCP/IP standard imposes a layered communications system structure. All the layers are located on each computer in the network, and each module or layer is a separate component that theoretically functions independent of the other layers.

TCP/IP and its related protocols form a standardized system for defining how data should be processed, transmitted and received on the Internet. TCP/IP defines the network communication process, and more importantly, defines how a unit of data should look and what information the message should contain so that the receiving computer can interpret the message correctly. Because the standardized layer design of TCP/IP, a consistent conversion of base data is ensured regardless of the version or vendor of the TCP/IP conversion software.

TCP/IP Addressing and Routing

A computer operating on a network is assigned a unique physical address. On a Local Area Network ("LAN"), the physical address of the computer is a number given to computer's network adapter card. Hardware LAN protocols use this physical address to deliver packets of data to computers on the LAN.

On the Internet, the TCP/IP protocol routes information packets using logical addressing. The network software in the Network Layer generates logical addresses. Specifically, a logical address in the TCP/IP network is translated into a corresponding physical address using the ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol) protocols in the Network Layer.

The TCP/IP's logical address is also called an IP address. The IP address can include: (1) a network ID number identifying a network, (2) a sub-network ID number identifying a sub-network on the network, and,

(3) a host ID number identifying a particular computer on the sub-network. The header data in the information packet will include source and destination addresses. The IP addressing scheme imposes a sensible addressing scheme that reflects the internal organization of the network or sub-network.

A computer network is often subdivided into smaller sub-networks. The computer network is divided in this manner to increase data transmission efficiency and reduce overall network traffic. Routers are used to regulate the flow of data into and out of designated sub-networks of the computer network.

A router interprets the logical address information of a data packet, such as an IP address, and directs the data packet across the network to its intended destination. Data addressed between computers on the sub-network does not pass through the router to the greater network, and therefore does not clutter the transmission lines of the greater network. If data is addressed to a computer outside the sub-network, however, the router forwards the data onto the larger network.

The TCP/IP network includes protocols that define how routers will determine the path for data through the network. Routing decisions are based upon information in the IP packet header and entries in each router's routing table. A routing table possesses sufficient information for a router to make a determination on whether to accept the communicated information on behalf of a destination computer, or pass the information onto another router in the network. The routing table also permits the router to determine where the information should be forwarded within the network or sub-network.

The routing table can be configured manually with routing table entries or a dynamic routing protocol that can accommodate changing network topologies – network architecture or network layouts, routers, and interconnections between hosts and routers. In a dynamic routing protocol, a router advertises reachability when it sends updated routing

information to a second router claiming that the first router is capable of reaching one or more destination addresses. Advertising accessibility is important to the process of receiving, directing and re-directing data packets on the Internet.

5 Confidential Communications Over a Public Network

Because information packets are routed over the public networks that make up the Internet, cryptographic security systems are used to send communications in a confidential manner. These security systems maintain the confidentiality of the information packet by encoding, or
10 encrypting, the information in the information packet. The encryption process can only be reversed, or decoded, by an authorized person. Other activities performed by the security system include authentication (you are who you say you are), integrity checking (the information packet was sent in the decoded form) and non-repudiation (identification of person sending
15 the information packet).

A cryptographic security system consists of two fundamental components -- a complicated mathematical algorithm for encrypting the information, and one or more values, called keys, known to parties authorized to transmit or receive the information packet. The greater the
20 complexity of the algorithm, the stronger the cryptographic level of security in the cryptographic system. Because of its complexity, the algorithm can be kept secret or publicly disclosed without undermining the strength of the security system.

As an example of the encryption process, let's examine the
25 situation where Party A intends to communicate confidentially with Party B using the cryptographic security system. First, Party A uses the algorithm and a key to transform the information in the transmitted information packet into encrypted information. In order to maintain the confidentiality of the transmitted information, the encrypted information
30 does not resemble the information in the information packet, and the

encrypted information cannot be easily decoded into its original form without the use of the algorithm and a key.

As such, the encrypted information is transmitted over the public networks on the Internet to Party B without disclosing the content of the original information packet. After receiving the encrypted information packet, Party B decodes the encrypted information using the algorithm and a key. When the encrypted information is decoded, the original information should be disclosed in the decoded information packet.

Key-Based Cryptographic Systems

It is preferable that the key be known only to the appropriate or authorized parties to the communication. This type of key is known as a “secret key”, and the sender and receiver of the information packet use the same secret key to encrypt and decode information packets with the algorithm. Public key encryption is also supported by cryptographic security systems where the sender has a public key and a private key, and the receiver has a public key and a private key. Messages may be encoded by the sender using the receiver’s public key, and decoded by the receiver using the receiver’s private key. Hybrid security systems are also used to encrypt and decode information in information packets. Accordingly, key-based security systems rely on the use of some type of secret key to support confidential communications.

SUMMARY OF THE INVENTION

Internet protocols were originally developed with an assumption that Internet users, which are assigned a unique IP address, would be connected to a single, fixed network – that is, one physical fixed location. With the advent of portable computers and cellular wireless communication systems, however, the movement of Internet users within a network and across network boundaries has become quite common. Because of this highly mobile Internet usage, the implicit design assumptions for the Internet protocols have been violated.

The IP-Based Mobile System

The IP-based mobile system includes at least one Mobile Node in a wireless communication system. The term "Mobile Node" includes a mobile communication unit, and, in addition to the Mobile Node, the communication system has a home network and a foreign network. The Mobile Node may change its point of attachment to the Internet through these other networks, but the Mobile Node will always be associated with a single Mobile Node home network for IP addressing purposes.

The home network has a Home Agent and the foreign network has a Foreign Agent -- both of which control the routing of information packets into and out of their network. The terms Home Agent and Foreign Agent may be defined in the Mobile IP Protocol (RFC 2002), but these agents are not restricted to a single protocol or system. In fact, the term Home Agent, as used in this application, can refer to a Home Mobility Manager, Home Location Register, Home Serving Entity, or any other agent at a home network having the responsibility to manage mobility-related functionality for a Mobile Node on a home network. Likewise, the term Foreign Agent, as used in this application, can refer to a Serving Mobility Manager, Visited Location Register, Visiting Serving Entity, or any other agent on a foreign network having the responsibility to manage mobility-related functionality for a Mobile Node on a foreign network.

Security System for the IP-Based Mobile System

In an IP-based mobile communications system, the Mobile Node changes its point of attachment to the network while maintaining network connectivity. Security concerns arise in the mobile system because authorized users are subject to the following forms of attack: (1) session stealing where a hostile node hijacks the network session from mobile node by redirecting information packets, (2) spoofing where the identity of an authorized user is utilized in an unauthorized manner to obtain access to the network, and (3) eavesdropping and stealing of information during a

session with an authorized user. No separate secure network exists in the IP-based mobility communications system, and therefore, it is necessary to protect information transmitted in the mobile system from the above-identified security attacks.

5 The present invention improves the security of communications in a IP-based mobile communications system by creating variable-based Security Associations (SAs) between various nodes on the system, a Virtual Private Network supported by a Service Level Agreement (SLA) between various foreign networks and a home network, and an SLA
10 Broker to promote large-scale roaming among different SLAs supported by the SLA Broker or agreements with other SLA Brokers. Any one of these aspects will improve the security of the system, and each aspect is independently covered by the present invention.

Variable-Based Security Associations

15 Security Associations, called SAs, are relationships between secure nodes, or routers, of the Internet. The present invention establishes SAs between various nodes and agents on the system to comprehensively, and flexibly, cover connections in the network.

Service Level Agreements (SLAs) and Virtual Private Networks (VPNs)

20 A service level agreement (SLA) may be created between networks on the Internet to establish Security Associations between Authentication, Authorization, and Accounting (“AAA”) servers on various administrative domains or networks. The AAA servers on the SLAs can assist in the management of SAs and the uniform transfer of
25 encrypted information packets between AAA servers using a well-defined security protocol.

 An SLA can be formed between the AAA servers on several foreign networks and a home network. By working cooperatively, the AAA servers form a secure network for communications. Essentially, this
30 system forms a Virtual Private Network (or “VPN”) between the foreign

networks and the home network thereby supporting secure tunneling of information packets among the networks on the VPN.

SLA Brokers

To eliminate the need for each network to establish individual SLA's with every other service provider and network on the Internet, SLA brokers can be assigned the responsibility of establishing and maintaining SLAs found on different networks (and reciprocal agreements with other SLAs and SLA Brokers). Accordingly, the SLA Broker becomes a consortium of agreements between various networks and service providers.

A home network need only establish one relationship with the SLA Broker in order to gain access to the other SLAs supported by the SLA Broker. With the support of such an SLA Broker, a mobile node from the home network can roam about any other network supported by the home network's SLA Broker.

While the present invention can operate under the Mobile IP (RFC 2002), IPSec, and/or Internet Key Exchange (IKE) protocols, the invention is not limited to these protocols and can be used with any IP-based mobile system and associated security protocols.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects and features of the invention will become more readily understood from the following detailed description and appended claims when read in conjunction with the accompanying drawings in which like numerals represent like elements and in which:

Fig. 1 is a schematic diagram of the various SAs supported in the security framework;

Fig. 2 is a message flow sequence for establishing an SA;

Fig. 3 is a schematic diagram of the Virtual Private Network created by a common Service Level Agreement; and,

Fig. 4 is a schematic diagram showing the SLA Broker in the network configuration.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Mobile IP protocols support the routing of data communications to Mobile Nodes on the Internet. For the most part, each Mobile Node in a mobile IP system is identified by a permanent IP address associated with a home network. While the Mobile Node is coupled to its home network, the Mobile Node functions as any other fixed node on that network. When the Mobile Node moves from its home network to a foreign network, however, the home network sends data communications to the Mobile Node through the foreign network. This transmission of the information packet from the home network to the foreign network is called “tunneling” the information packet to the foreign network and/or mobile foreign network where the mobile user is located.

Variable-Based Security Associations

In order to reduce the security concerns during the “tunneling” of information packets to Mobile Nodes, different security associations can be formed between home and foreign networks. Security Associations, called SAs, are relationships between secure nodes, or routers, in the security framework of the Internet. The SA establishes the agreement between the two secure nodes on how the sender will cryptographically transform data before transmission.

The SA agreement requires the sending node to share information with the receiving node about the type of cryptographic method, the algorithm, and the keys used in the encryption process. The agreement is formed and the information is shared prior to the transmission of an information packet on the secure connection. When the sending node transmits an encrypted information packet, the sending node will identify the pertinent information regarding the encryption method to the receiving node. After receiving the encrypted information packet, the receiving node will use the shared information from the SA to decode the information packet.

Authentication is the process of proving someone's claimed identity, and security systems will often require authentication of the system user's identity before authorizing a requested activity. The authentication and authorization processes are often performed by an AAA server. The AAA server authenticates the identity of an authorized user, and authorizes the requested activity. Additionally, the AAA server will provide the accounting function including tracking usage and charges for use of secure transmissions links.

Looking at Figure 1, the overall architecture of the IP-based mobile system is shown with Mobile Node 64, home network 10 and foreign network 40. The home network 10 has a central buss line 20 coupled to the home agent 28 via communication link 24, and the buss line 20 is coupled to the secure messaging gateway 15 via communication link 22. The secure messaging gateway 15 includes the AAA server 17 and firewall 19 for the home network. The home network 10 is coupled to the public Internet 35 via communication link 30. A communications link is any connection between two or more nodes on a network or users on networks or administrative domains.

The foreign network 40 has a central buss line 50 coupled to the foreign agent 58 via communication link 54, and the buss line 50 is coupled to the secure messaging gateway 45 via communication link 52. The secure messaging gateway 45 includes the AAA server 49 and firewall 47 for the foreign network. The foreign network 40 is coupled to the public Internet 35 via communication link 37.

A Mobile Node 64 is shown electronically coupled to the foreign network 40 via the communication link 66 of transceiver 60. Transceiver 60 is coupled to the foreign network via communication link 62. The Mobile Node 64 can communicate with any transceiver or Access Network coupled to the foreign network 40. The system also includes a correspondent node CN 70, which is a node wishing to communicate with

the Mobile Node 64. The correspondent node CN 70 is coupled to the public Internet 35 via communication link 72.

The present invention includes the capability of forming five different SAs securely connecting various nodes and routers on the Internet. The following security associations will connect the following nodes and routers:

(1) SA1 - the SA1 80 securely connects the secure messaging gateway 15 in the home network 10 to the secure messaging gateway 45 in the foreign network 40,

(2) SA2 - the SA2 85 securely connects the Mobile Node 64 to the Foreign Agent 58 in the foreign network 40,

(3) SA3 - the SA3 87 securely connects the Mobile Node 64 to the Home Agent 28 in the home network 10,

(4) SA4 - the SA4 90 securely connects the Mobile Node 64 to the correspondent node 70, and

(5) SA5 - the SA5 92 securely connects the correspondent node 70 to the Home Agent 28 in the home network.

The security scheme in the present invention covers one or more portions of the public network as mandated by the needs of the user and the level of security desired. At the very least, SA1 80 is needed to traverse the public networks in the Internet. If SA1 80 and SA2 85 (or an equivalent) are available and the foreign network 40 can be trusted, SA3 would be optional because it would cover redundant relationships already covered by SA1 and SA2. Further, SA4 is only needed if the policies at the Mobile Node 64 require its use. If SA1 80 is not available, the system should secure transmission of information packets by using SA3 87 and SA4 90 between the Mobile Node 64 and the Home Agent 28 or correspondent node 70, respectively. SA2 connection may be unnecessary if the Mobile Node 64 communicates with the Foreign Agent 58 using a code-based communication scheme, such as a CDMA-based communication scheme. Further, the security of the system could be

enhanced by SA5 92 between the correspondent node 70 and the Home Agent 28 if the correspondent node 70 is not associated with the home network.

Many combinations of the SAs could be established to provide a comprehensive security framework. Of course, redundant SAs can be eliminated, such as the SA3 connection where there is already SA1 and SA2 connections available for use. As a flexible solution, the SAs available in the present invention could be configured by the user or the networks to provide the desired level of security.

Registration and AAA Redirection

Foreign Agents and Home Agents periodically broadcast an agent advertisement to all nodes on the local network associated with that agent. An agent advertisement is a message from the agent on a network that may be issued under the Mobile IP protocol (RFC 2002) or any other type of communications protocol. This advertisement should include information that is required to uniquely identify a mobility agent (e.g. a Home Agent, a Foreign Agent, etc.) to a mobile node. Mobile nodes examine the agent advertisement and determine whether the mobile node is connected to its home network or a foreign network.

If the mobile node is located on its home network, no additional actions need to be taken because information packets will be routed to the node according to the standard addressing and routing scheme. If the mobile node is visiting a foreign network, however, the mobile node obtains a care-of address from the agent advertisement, and registers this care-of address with its Home Agent. The care-of address identifies the foreign network where the mobile node is located. The Home Agent uses this care-of address to tunnel data packets to the foreign network for subsequent transfer to the mobile node.

To enhance security using the present invention, mobility related messages, sometimes called control or control plane messages, transmitted between the foreign and home agents should be directed through the local

AAA servers on the respective networks. This includes the AAA server 17 on the home network 10 and the AAA server 49 on the foreign network 48. Every time the Mobile Node 64 moves into a new foreign network or powers up in the foreign network, the Mobile Node 64 must negotiate a new secure SA2 85 connection with the Foreign Agent 58. While the control plane messages should be redirected through the AAA servers in the home and foreign networks, the SA2 85 connection will only be initiated after the registration request and registration response have been initially sent outside a secure connection, also called "in the clear." That is, the Mobile Node 64 will first successfully register with the Foreign Agent 58 and the Home Agent 28 without the use of a secure connection. In order to establish the SA2 85 secure connection between the Mobile Node 64 and the Foreign Agent 58 thereafter, the registration request and response must be resent using the secure connection through the AAA servers on the home and foreign networks. Any subsequent registrations, after the initial registration, are done using the SAs established during the initial registration.

The establishment of the SA2 secure connection with the redirection of the registration request and response through the AAA servers can be seen in Figure 2 in steps 100 to 106 where the registration request from the Mobile Node 64 to the Foreign Agent 58 is shown in step 100, the registration request from the Foreign Agent 58 to the AAA server 49 at the foreign network 40 is shown in step 102, the registration request from the AAA server 49 at the foreign network 40 to the AAA server 17 at the home network 10 in step 104, and the registration request from the AAA server 17 on the home network 10 to the Home Agent 28 in step 106.

The redirection of the registration response through the AAA servers is shown in steps 110 to 116 where the registration response from Home Agent 28 to AAA server 17 on the home network 10 is shown in step 110, registration response from AAA server 17 on the home network

10 to AAA server 49 on the foreign network 40 is shown in step 112, registration response from the AAA server 49 on the foreign network 40 to the Foreign Agent 58 is shown in step 114, and registration response from the Foreign Agent 58 to the Mobile Node 64 is shown in step 116.

5 If the Foreign Agent 58 is capable of establishing an SA relationship, then the agent advertisement issued by the Foreign Agent 58 should be expanded to indicate this capability to the Mobile Node 64. The Mobile Node 64 can then initiate establishment of the secure connection, and it is recommended that the Aggressive Mode of the Internet Key
10 Exchange protocol (IKE) can be used as shown in step 120 of Figure 2. The Quick Mode in step 122 can also be used to speed the SA set-up operation as shown in Figure 2. Lastly, in order to enhance the registration process, the registration response from the Home Agent 28 to the Foreign Agent 58 can carry the public key associated with the Mobile
15 Node 64, and the response could also carry the public key of the Foreign Agent 58 from the Foreign Agent 58 to the Mobile Node 64.

 Some means should be used to authenticate the identity of the mobile user to the foreign agent. One method of authenticating a user identity is the use of x.509 certificates based upon a public key-based
20 system such as the Public Key Infrastructure (PKI). A cross certification scheme may also be used through a common Service Level Agreement between the home network and the foreign network. Digital signatures could also be used to authenticate the identity of a user to a foreign network. Public keys for the Mobile Node and the foreign network can
25 also be exchanged.

Service Level Agreements (SLAs) and Virtual Private Networks (VPNs)

 A service level agreement (SLA) can be created between networks on the Internet to establish Security Associations between Authentication, Authorization, and Accounting (“AAA”) servers on various networks. In
30 Figure 3, an SLA can exist between the home network 200 and the foreign

networks 215. Likewise, SLA may exist between the home network 200 and the foreign networks 235 and 255, respectively.

The home network 200 includes the secure messaging gateway 202 with the AAA server 204. The secure messaging gateway 202 couples the home network 200 to the Internet 210 via communication link 206. The foreign network 215 to the Internet 210 includes the secure messaging gateway 225 with the AAA server 220. The secure messaging gateway 225 couples the foreign network 215 to the Internet 210 via communication link 230. The foreign network 235 includes the secure messaging gateway 240 with the AAA server 245. The secure messaging gateway 240 couples the foreign network 235 to the Internet 210 via communication link 250. The foreign network 255 includes the secure messaging gateway 260 with the AAA server 265. The secure messaging gateway 260 couple the foreign network 255 via communication link 275.

The AAA servers 204, 220, 245 and 265 can assist in the management of SAs and support the uniform transfer of encrypted information packets using a well-defined security protocol. An SLA can be established between the AAA servers on the several foreign networks 215, 235 and 255 and home network 200. The secure messaging gateways 202, 225, 240 and 260 also play the role as security gateway (firewall functions) for their respective network.

Routing devices know the existence of an AAA server 204, 220, 245 and 265 on a network, and all information packets transmitted in a secure mode should be routed through this routing device. One AAA server 204, 220, 245 and 265 then communicates with another AAA server on the network via a confidential communication link. By working cooperatively, the AAA servers 204, 220, 245 and 265 form a secure network for communications. Essentially, this system of SAs uses a single SLA to form a Virtual Private Network (or "VPN") between the foreign networks 215, 235 and 255 and the home network 200 thereby supporting secure tunneling of information packets among the networks on the VPN.

Because a single SLA supports the networks 200, 215, 235 and 255 in the VPN shown in Figure 3, a mobile node can roam among these networks 200, 215, 235, and 255 and securely access the network at any point in the VPN.

5 The AAA servers 204, 220, 245 and 265 in the VPN shown in Figure 3 support the security gateways 202, 225, 240 and 260 for the networks 200, 215, 235 and 255, respectively. The home agents and foreign agents on the networks are aware of the AAA servers 204, 220, 245 and 265, and route the control plane messages through the AAA
10 servers to ensure confidential communications. Policies configured at the home agent, foreign agents, or the AAA servers 204, 220, 245 and 265 indicate how the Mobile Nodes will use these secure tunnels for message transfer. The home network for the Mobile Node can also be identified from the registration request.

15 Secure communication links between the AAA servers 204, 220, 245 and 265 will remain in place as long as the SLAs are valid. The AAA servers 220, 245 and 265 in the foreign networks 215, 235, and 255 and AAA server 204 in the home network 200 are configured with appropriate security policies that aid in the establishment of this SA. The present
20 invention provides a security framework for control plane messages between different domains as the Mobile Node roams throughout the VPN.

SLA Brokers

25 Establishing multiple SLAs among multiple service providers and networks increases the management complexity of the system. In order to reduce this management complexity and allow large-scale roaming among different networks, SLA Brokers can be established to provide a common support platform for multiple SLAs. The SLA Broker essentially becomes a consortium of SLAs from various networks, and Mobile Nodes need
30 only have a relationship with a single SLA maintained by an SLA Broker to acquire indirect access to other SLAs through the reciprocal agreements

with other SLAs maintained by the SLA Broker (and indirectly other SLA Brokers). By allowing access to all SLAs in a network, the Mobile Node can roam throughout the networks without having to establish independent relationships with the other SLAs.

5 In Figure 4, the home network 310 supports a secure messaging gateway 315 having an AAA server 317 and firewall 319. The secure messaging gateway 315 is coupled to the home network common buss line 320 via communication link 322. The home network 310 has a home agent 328 that is coupled to the home network communication buss 320
10 via communication link 324. The home network 310 is coupled to the public Internet 335 via communication link 330.

The foreign network 340 supports a secure messaging gateway 345 having an AAA server 349 and firewall 347. The secure messaging gateway 345 is coupled to the home network common buss line 350 via
15 communication link 352. The foreign network 340 has a foreign agent 358 that is coupled to the foreign network communication buss 350 via communication link 354. The foreign network 340 is coupled to the public Internet 335 via communication link 337. The Mobile Node 364 communicates with the network via the cellular transceiver 360 (or any
20 other type of Access Network coupled to the foreign network 340), which is coupled to the Foreign Agent 358 via communication link 362.

After moving to the foreign network 340 or upon power-up at that network and under the condition that no SLA exists between the foreign network 340 and the home network 310, the Mobile Node 364 will first
25 send a registration request message to the Foreign Agent 358. The registration request and response may be sent initially in the clear to establish the relationship, but the registration request and response must be re-established later in a secure connection. In order to establish this
30 secure connection, the Foreign Agent 358 forwards the registration request to the foreign AAA server 349, and the AAA server 349 looks at the address of the mobile node 364 from the registration request to confirm

whether an SLA exists between the home network 310 and the foreign network 340. Thereafter, any registration requests and responses are established using the secure connection established initially according to the procedure described above.

5 After confirming that no SLA exists between the home network 310 and foreign network 340, the AAA server 349 consults with the SLA Broker 375 in communication 380. If the SLA Broker 375 is associated with the home network 310, the SLA Broker 375 sends a response 385 to the AAA server 349 with a session key that is generated to establish the
10 SLA between the foreign and home networks. At the same time, the SLA Broker 375 sends the same session key to the AAA server 317 in the home network 310 in a different message (not shown in figure). The session key should be transmitted to the AAA servers 349 and 317 over secure communications links.

15 Certificates can also be used to authenticate the registration request and response protocol, where a certificate contains appropriate identification information to authenticate the identity of the networks, administrative domains and users. The SLA Broker 375 may return a certificate to the foreign AAA server 349 that is sent to the AAA server
20 317 at the home network 310 via the registration request. Since the home AAA server 317 has an SLA with the SLA Broker 375, the certificate presented by the foreign network 340 can be accepted and a successful registration response is returned. In this manner, the secure communication link between the SAs can also be established.

25 In the response to communication 385, the AAA server 349 in the foreign network 340 is also passed the IP address of the AAA server 317 in the home network. The AAA server 349 initiates a key encryption negotiation 390 with the AAA server 317 in the home network 310. The session key given by the SLA Broker 375 would be used for
30 authentication purposes. Once the SA is set up, the messages between the

5

1990
 1991
 1992
 1993
 1994
 1995
 1996
 1997
 1998
 1999
 2000
 2001
 2002
 2003
 2004
 2005
 2006
 2007
 2008
 2009
 2010
 2011
 2012
 2013
 2014
 2015
 2016
 2017
 2018
 2019
 2020
 2021
 2022
 2023
 2024
 2025
 2026
 2027
 2028
 2029
 2030
 2031
 2032
 2033
 2034
 2035
 2036
 2037
 2038
 2039
 2040
 2041
 2042
 2043
 2044
 2045
 2046
 2047
 2048
 2049
 2050
 2051
 2052
 2053
 2054
 2055
 2056
 2057
 2058
 2059
 2060
 2061
 2062
 2063
 2064
 2065
 2066
 2067
 2068
 2069
 2070
 2071
 2072
 2073
 2074
 2075
 2076
 2077
 2078
 2079
 2080
 2081
 2082
 2083
 2084
 2085
 2086
 2087
 2088
 2089
 2090
 2091
 2092
 2093
 2094
 2095
 2096
 2097
 2098
 2099
 2100
 2101
 2102
 2103
 2104
 2105
 2106
 2107
 2108
 2109
 2110
 2111
 2112
 2113
 2114
 2115
 2116
 2117
 2118
 2119
 2120
 2121
 2122
 2123
 2124
 2125
 2126
 2127
 2128
 2129
 2130
 2131
 2132
 2133
 2134
 2135
 2136
 2137
 2138
 2139
 2140
 2141
 2142
 2143
 2144
 2145
 2146
 2147
 2148
 2149
 2150
 2151
 2152
 2153
 2154
 2155
 2156
 2157
 2158
 2159
 2160
 2161
 2162
 2163
 2164
 2165
 2166
 2167
 2168
 2169
 2170
 2171
 2172
 2173
 2174
 2175
 2176
 2177
 2178
 2179
 2180
 2181
 2182
 2183
 2184
 2185
 2186
 2187
 2188
 2189
 2190
 2191
 2192
 2193
 2194
 2195
 2196
 2197
 2198
 2199
 2200
 2201
 2202
 2203
 2204
 2205
 2206
 2207
 2208
 2209
 2210
 2211
 2212
 2213
 2214
 2215
 2216
 2217
 2218
 2219
 2220
 2221
 2222
 2223
 2224
 2225
 2226
 2227
 2228
 2229
 2230
 2231
 2232
 2233
 2234
 2235
 2236
 2237
 2238
 2239
 2240
 2241
 2242
 2243
 2244
 2245
 2246
 2247
 2248
 2249
 2250
 2251
 2252
 2253
 2254
 2255
 2256
 2257
 2258
 2259
 2260
 2261
 2262
 2263
 2264
 2265
 2266
 2267
 2268
 2269
 2270
 2271
 2272
 2273
 2274
 2275
 2276
 2277
 2278
 2279
 2280
 2281
 2282
 2283
 2284
 2285
 2286
 2287
 2288
 2289
 2290
 2291
 2292
 2293
 2294
 2295
 2296
 2297
 2298
 2299
 2300
 2301
 2302
 2303
 2304
 2305
 2306
 2307
 2308
 2309
 2310
 2311
 2312
 2313
 2314
 2315
 2316
 2317
 2318
 2319
 2320
 2321
 2322
 2323
 2324
 2325
 2326
 2327
 2328
 2329
 2330
 2331
 2332
 2333
 2334
 2335
 2336
 2337
 2338
 2339
 2340
 2341
 2342
 2343
 2344
 2345
 2346
 2347
 2348
 2349
 2350
 2351
 2352
 2353
 2354
 2355
 2356
 2357
 2358
 2359
 2360
 2361
 2362
 2363
 2364
 2365
 2366
 2367
 2368
 2369
 2370
 2371
 2372
 2373
 2374
 2375
 2376
 2377
 2378
 2379
 2380
 2381
 2382
 2383
 2384
 2385
 2386
 2387
 2388
 2389
 2390
 2391
 2392
 2393
 2394
 2395
 2396
 2397
 2398
 2399
 2400
 2401
 2402
 2403
 2404
 2405
 2406
 2407
 2408
 2409
 2410
 2411
 2412
 2413
 2414
 2415
 2416
 2417
 2418
 2419
 2420
 2421
 2422
 2423
 2424
 2425
 2426
 2427
 2428
 2429
 2430
 2431
 2432
 2433
 2434
 2435
 2436
 2437
 2438
 2439
 2440
 2441
 2442
 2443
 2444

CLAIMS

1. A method for securely communicating to a mobile node on a communications system having a home network for the mobile node and at least one foreign network comprising the steps of:
 - establishing at least one security association between the
 - 5 home network and the foreign network;
 - establishing at least one security association between the mobile node and the foreign network;
 - encrypting information in an information packet to be transmitted from the mobile node to the home network;
 - 10 transmitting the information packet from the mobile node using the security associations to support secure communications from the mobile node;
 - decoding information from the encrypted information packet at the home network to retrieve the information.
2. The method of securely communicating to a mobile node in Claim 1 further comprising the step of:
 - establishing a security association between the home network and a correspondent node.
3. The method of securely communicating to a mobile node in Claim 1 further comprising the step of:
 - establishing a security association between the mobile node and a correspondent node.
4. The method of securely communicating to a mobile node in Claim 3 further comprising the step of:
 - establishing a security association between the home network and a correspondent node.

5. The method of securely communicating to a mobile node in Claim 1 further comprising the step of:
encrypting information using a public key algorithm.
6. The method of securely communicating to a mobile node in Claim 1 further comprising the step of:
encrypting information using a private key algorithm.
7. The method of securely communicating to a mobile node in Claim 1 further comprising the step of:
supporting the secure communication for the security association between the foreign network and the mobile node using a code-based cellular communication system.
8. The method of securely communicating to a mobile node in Claim 1 further comprising the step of:
establishing multiple security associations between a plurality of foreign networks and the home network.
9. The method of securely communicating to a mobile node in Claim 8 further comprising the step of:
establishing a service level agreement to manage the secure communication of information packets on the multiple security associations.
10. The method of securely communicating to a mobile node in Claim 9 further comprising the step of:
establishing a broker to assist in the use of service level agreements on the secure communications system.

11. A method for securely communicating to a mobile node on a communications system having a home network for the mobile node and at least one foreign network comprising the steps of:

- 5 establishing at least one security association between the home network and the mobile node;
- encrypting information in an information packet to be transmitted from the mobile node to the home network;
- transmitting the information packet from the mobile node
- 10 using the security associations to support secure communications from the mobile node;
- decoding information from the encrypted information packet at the home network to retrieve the information.

12. The method of securely communicating to a mobile node in Claim 11 further comprising the step of:

 establishing a security association between the home network and a correspondent node.

13. The method of securely communicating to a mobile node in Claim 11 further comprising the step of:

 the step of a security association between the mobile node and a correspondent node.

14. The method of securely communicating to a mobile node in Claim 13 further comprising the step of:

 establishing a security association between the home network and a correspondent node.

15. The method of securely communicating to a mobile node in Claim 11 further comprising the step of:

encrypting information using a public key algorithm.

16. The method of securely communicating to a mobile node in Claim 11 further comprising the step of:

encrypting information using a private key algorithm.

17. The method of securely communicating to a mobile node in Claim 11 further comprising the step of:

establishing multiple security associations between a plurality of foreign networks and the home network.

18. The method of securely communicating to a mobile node in Claim 17 further comprising the step of:

establishing a service level agreement to manage the secure communication of information packets on the multiple security associations.

19. The method of securely communicating to a mobile node in Claim 18 further comprising the step of:

establishing a broker to assist in the use of service level agreements on the secure communications system.

20. A system for securely communicating to a mobile node in a wireless communications network comprising:

a home network having a home agent coupled to a router capable of directing information packets to and from the home network;

a foreign network having a foreign agent coupled to a router capable of directing information packets to and from the foreign network and a transceiver capable of performing wireless communications with at least one mobile node in the transmission range of the transceiver for the foreign network;

a security association established between the home network and the foreign network and a security association established between the mobile node and the foreign network, both security associations used to support the secure communication of information packets from the mobile node to the home network.

21. The system of securely communicating to a mobile node in Claim 20 further comprising:

a security association between the home network and a correspondent node.

22. The system of securely communicating to a mobile node in Claim 20 further comprising:

a security association between the mobile node and a correspondent node.

23. The system of securely communicating to a mobile node in Claim 22 further comprising:

a security association between the home network and a correspondent node.

24. The system of securely communicating to a mobile node in Claim 20 further comprising:

a public key encryption means to secure communications.

25. The system of securely communicating to a mobile node in Claim 20 further comprising:

a private key encryption means to secure communications.

26. The system of securely communicating to a mobile node in Claim 20 further comprising:

multiple security associations between a plurality of foreign networks and the home network.

27. The system of securely communicating to a mobile node in Claim 26 further comprising:

a service level agreement to manage the secure communication of information packets on the multiple security associations.

28. The system of securely communicating to a mobile node in Claim 27 further comprising:

a broker to assist in the use of service level agreements on the secure communications system.

29. A system for securely communicating to a mobile node in a wireless communications network comprising:

a home network having a home agent coupled to a router capable of directing information packets to and from the home network;

a foreign network having a foreign agent coupled to a router capable of directing information packets to and from the foreign network and a transceiver capable of performing wireless communications with at least one mobile node in the transmission range of the transceiver for the foreign network;

a security association established between the home network and the mobile node, the security association used to support the secure communication of information packets from the mobile node to the home network.

30. The system of securely communicating to a mobile node in Claim 29 further comprising:

a security association between the home network and a correspondent node.

31. The system of securely communicating to a mobile node in Claim 29 further comprising:

a security association between the mobile node and a correspondent node.

32. The system of securely communicating to a mobile node in Claim 31 further comprising:

a security association between the home network and a correspondent node.

33. The system of securely communicating to a mobile node in Claim 29 further comprising:

a public key encryption means to secure communications.

34. The system of securely communicating to a mobile node in Claim 29 further comprising:

a private key encryption means to secure communications.

35. The system of securely communicating to a mobile node in Claim 29 further comprising:

multiple security associations between a plurality of foreign networks and the home network.

36. The system of securely communicating to a mobile node in Claim 35 further comprising:

a service level agreement to manage the secure communication of information packets on the multiple security associations.

37. The system of securely communicating to a mobile node in Claim 36 further comprising:

a broker to assist in the use of service level agreements on the secure communications system.

SECURITY FRAMEWORK FOR IP MOBILITY SYSTEMS USING VARIABLE-BASED SECURITY ASSOCIATIONS AND BROKER REDIRECTION

ABSTRACT

In an IP-based mobile communications system, the Mobile Node changes its point of attachment to the network while maintaining network connectivity. Security concerns arise in the mobile system because authorized users are subject to the following forms of attack: (1) session stealing where a hostile node hijacks session from mobile node by redirecting packets, (2) spoofing where the identity of an authorized user is utilized in an unauthorized manner to obtain access to the network, and (3) eavesdropping and stealing of data during session with authorized user. No separate secure network exists in the IP-based mobility communications system, and therefore, it is necessary to protect information transmitted in the mobile system from the above-identified security attacks.

The present invention improves the security of communications in a IP mobile communications system by creating variable-based Security Associations between various nodes on the system, a Virtual Private Network supported by an Service Level Agreement between various foreign networks and a home network, and an SLA Broker to promote large-scale roaming among different SLAs supported by the SLA Broker or agreements with other SLA Brokers.

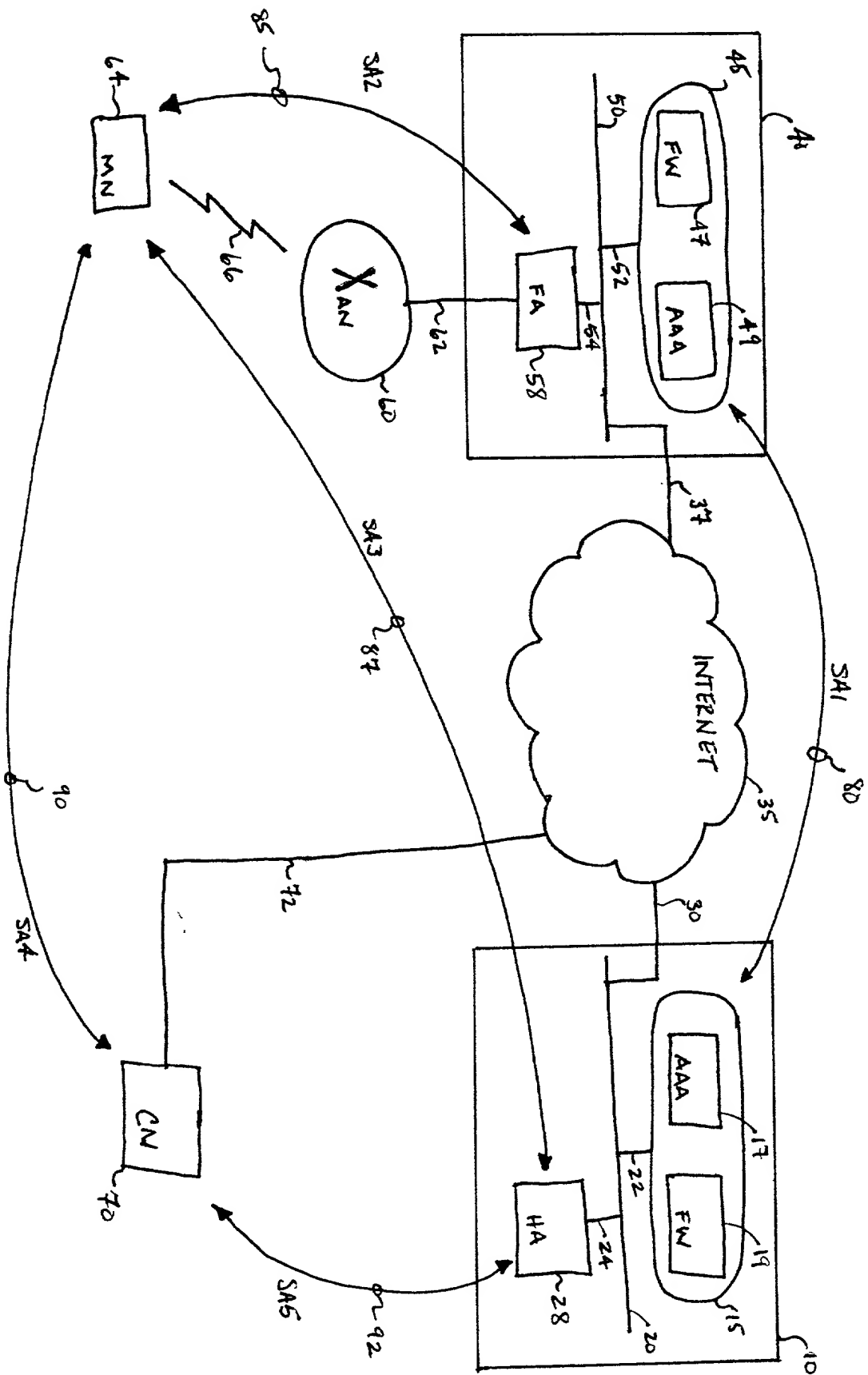


FIGURE 1

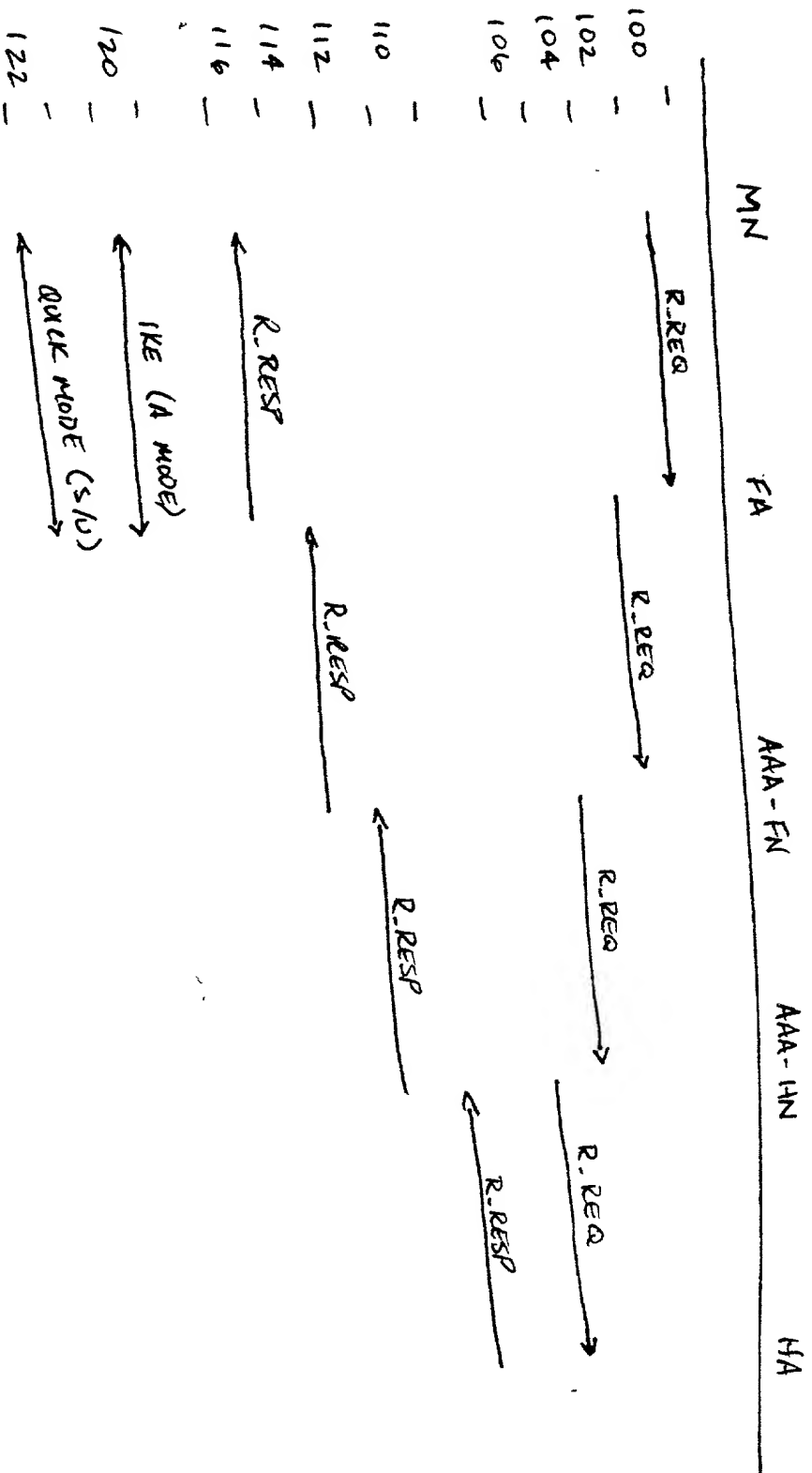
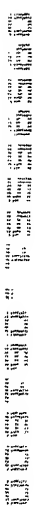


FIGURE 2



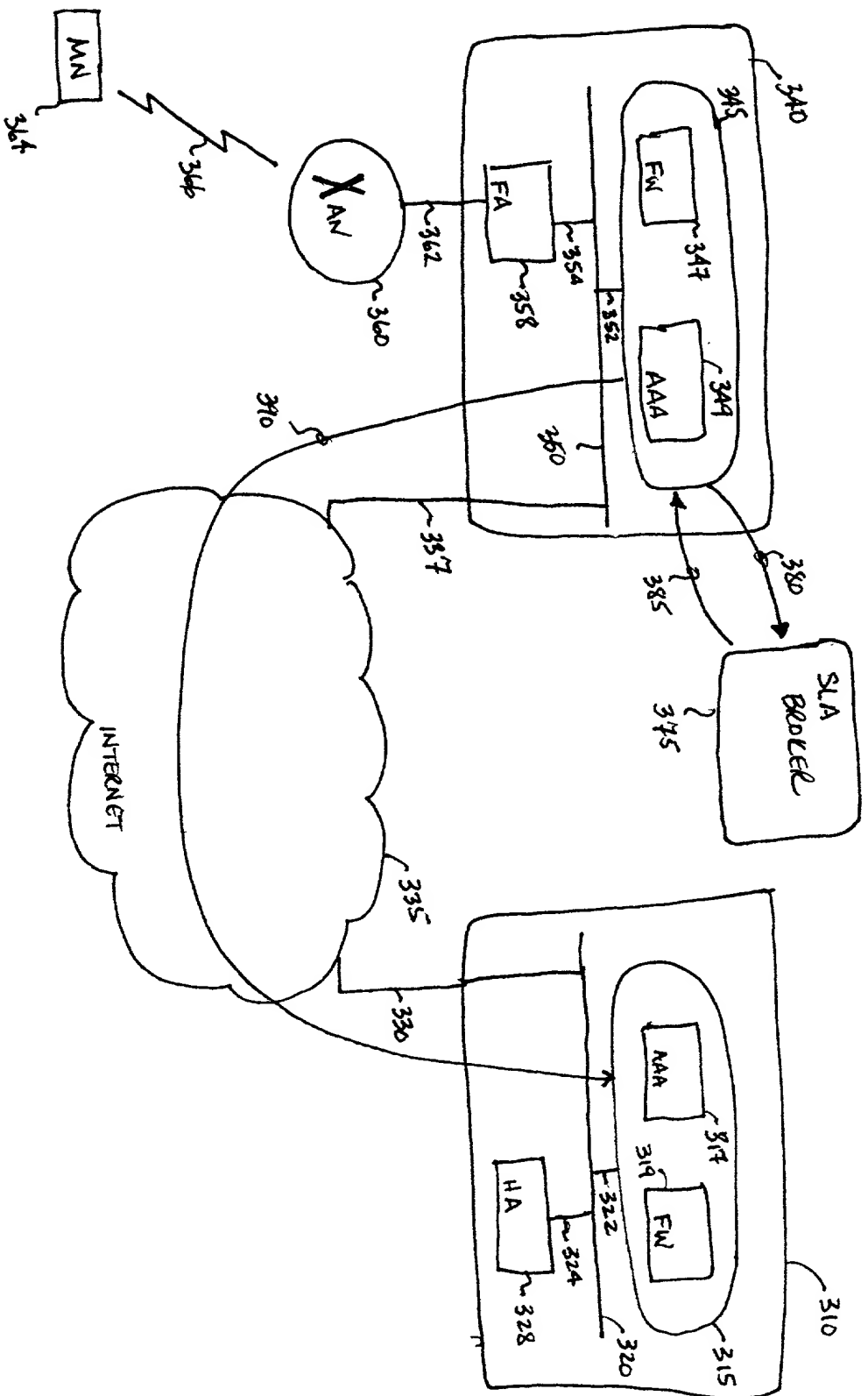


FIGURE 4

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL,
DIVISIONAL, CONTINUATION OR C-I-P)

As a below named inventor, we hereby declare that:

TYPE OF DECLARATION

This declaration is of the following type: (check one applicable item below)

- X original
design
supplemental

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below next to my name.
I believe I am the original, first and joint inventor of the subject matter which is claimed and for
which a patent is sought on the invention entitled:

TITLE OF INVENTION

**SECURITY FRAMEWORK FOR IP MOBILITY SYSTEMS USING VARIABLE-BASED
SECURITY ASSOCIATIONS AND BROKER REDIRECTION**

SPECIFICATION IDENTIFICATION

the specification of which: (complete (a), (b) or (c))

- (a) x is attached hereto.
- (b) was filed on _____ as Serial No. 08/ _____
or Express Mail No., as Serial No. not yet known
and was amended on _____ (if applicable)
- (c) was described and claimed in PCT International Application No.
filed on _____ and as amended under PCT Article
19 on _____ (if any).

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information

X which is material to patentability as defined in 37, Code of Federal Regulations, § 1.56

X and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable examiner would consider it important in deciding whether to allow the application to issue as a patent, and

In compliance with this duty there is attached an information disclosure statement in accordance with 37 CFR 1.98.

PRIORITY CLAIM (35 U.S.C. § 119)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

(complete (d) or (e))

(d) X no such applications have been filed.

(e) such applications have been filed as follows.

PRIOR FOREIGN/PCT APPLICATION(S) FILED WITHIN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119

COUNTRY (OR INDICATE IF PCT)	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 37 USC 119
			YES NO
			YES NO

ALL FOREIGN APPLICATIONS(S), IF ANY FILED MORE THAN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

POWER OF ATTORNEY

I hereby appoint the following attorney(s) and/or agents(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (List name and registration number)

D. Scott Hemingway (Reg. No. 36,366), John D. Crane (Reg. No. 25,231), Howard R. Greenberg (Reg. No. 26,171), W. Glen Johnson (Reg. No. 39,525), Randall W. Mishler (Reg. No. 42,006), Kevin L. Smith (Reg. No. 38,620), Vernon E. Williams (Reg. No. 38,713)

Attached as part of this declaration and power of attorney is the authorization of the above-named attorney(s) to accept and follow instructions from my representatives(s).

SEND CORRESPONDENCE TO DIRECT TELEPHONE CALLS TO:

D. Scott Hemingway, PC
Preston Plaza Tower, Suite 800
8300 Douglas Ave.
Dallas, TX 75225

(Name and telephone number)

D. Scott Hemingway
(214) 706-9082

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Full name of first joint inventor

Basavaraj B. Patil

Inventor's signature _____

Date _____ Country of Citizenship India

Residence: 7616 Capella Ct., Plano, TX 75025

Full name of second joint inventor

Raja P. Narayanan

Inventor's signature _____

Date _____ Country of Citizenship India

Residence: 4743 N. O'Connor Rd., Apt. 1026, Irving, TX 75062

Full name of third joint inventor

Haseeb Akhtar

Inventor's signature _____

Date _____ Country of Citizenship United States

Residence: 3102 Pamela Place, Garland, TX 75044

Full name of fourth joint inventor

Emad A. Qaddoura

Inventor's signature _____

Date _____ Country of Citizenship United States

Residence: 1320 Wateredge Dr., Plano, TX 75093